

**IN THE UNITED STATES DISTRICT COURT FOR THE
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

ALEX PRELIPCEANU, individually and)	
on behalf of similarly situated individuals,)	
)	
<i>Plaintiff,</i>)	Case No. 1:19-cv-00561
)	
v.)	
)	Honorable Robert W. Gettleman
JUMIO CORPORATION, a Delaware)	
Corporation.)	
)	JURY TRIAL DEMANDED
<i>Defendant.</i>)	
)	
_____)	

FIRST AMENDED COMPLAINT

Plaintiff Alex Prelipceanu, both individually and on behalf of similarly situated individuals, brings this First Amended Complaint against Defendant Jumio Corporation (“Jumio”), to put a stop to Defendant’s capture, collection, use, and storage of individuals’ biometric identifiers and/or biometric information in violation of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* (the “BIPA”), and to obtain redress for all persons injured by its conduct. Plaintiff alleges as follows based upon personal knowledge as to his own acts and experiences, and as to all other matters, upon information and belief, including an investigation conducted by his attorneys.

NATURE OF THE CASE

1. BIPA defines a “biometric identifier” as any personal feature that is unique to an individual, including fingerprints, palm scans and facial geometry. “Biometric information” is any information based on a biometric identifier, regardless of how it is converted or stored. 740 ILCS § 14/10. Collectively, biometric identifiers and biometric information are known as “biometrics.”

2. This case is about a cloud-based identity verification technology company capturing, collecting, storing, using and disseminating Plaintiff's and other consumers' biometric identifiers and/or biometric information without regard to BIPA and the concrete privacy rights and pecuniary interests that BIPA protects. Defendant collects consumers' biometric information in the form of facial geometry through software it provides to its customers that in turn requires consumers to undergo an identity and/or age verification process which relies on Defendant's software. Consumers who seek to purchase goods or services from Jumio's customers and subsequently undergo Jumio's identity verification are required to upload a driver's license, photo ID, or passport and are then required to upload a photo of themselves or otherwise undergo a scan of their facial geometry, often taken through a webcam. Defendant uses its NetVerify technology to extract the biometric facial geometry templates of these individuals and compare such biometric information to their photo ID. This allows for both identity verification and age verification, so the customer can proceed to potentially make purchases of both goods and services from the Defendant's customers' businesses.

3. Using its NetVerify ID & Age Verification System software, Defendant captures, stores and uses consumers' facial geometry and related biometric information without complying with BIPA's requirements.

4. Unlike ID badges or time cards – which can be changed or replaced if stolen or compromised – facial geometry is a unique and permanent biometric identifier associated with each consumer. This exposes consumers to serious and irreversible privacy risks. If for example, a database containing scans of face geometry or other sensitive, proprietary biometric data is hacked, breached, or otherwise exposed – like in ongoing and continuous data breaches –

consumers have no means by which to prevent identity theft, unauthorized tracking or other unlawful or improper use of this highly personal and private information.

5. In recognition of the concern over the security of individuals' biometrics, the Illinois Legislature enacted BIPA, specifically to regulate companies that collect and store Illinois citizens' biometrics, which provides, *inter alia*, that private entities, such as Defendant, may not collect, capture, purchase, or otherwise obtain an individual's biometric identifiers, such as facial geometry, or any biometric information, including any data regardless of the manner in which it is converted or stored, unless they first:

- a. inform that person in writing that biometric identifiers or biometric information will be collected or stored;
- b. inform that person in writing of the specific purpose and the length of term for which such biometric identifiers or biometric information is being collected, stored and used; and
- c. receive a written release from the person for the collection of their biometric identifiers or biometric information.

740 ILCS 14/15(b)(1)-(3).

6. BIPA also requires private entities in possession of biometric information to develop a publicly-available written policy outlining the storage and destruction policies of such biometric identifiers, and/or any biometric information derived from such identifiers. 750 ILCS 14/15(a).

7. Finally, private entities are prohibited from profiting from an individual's biometric identifiers or biometric information, as well as disclosing the same to third parties without informed consent. 740 ILCS 14/15(c)&(d).

8. Plaintiff brings this action for statutory damages and other remedies as a result of Defendant's conduct in violating his biometric privacy rights under BIPA.

9. Compliance with BIPA is straightforward and minimally-burdensome. For example, the necessary disclosures may be accomplished through a single sheet of paper.

10. BIPA's requirements bestow upon consumers a right to privacy in their biometrics and a right to make an *informed* decision when electing to provide or withhold his/her most sensitive information and on what terms.

11. BIPA's statutory scheme requires that private companies like Defendant make specific disclosures to consumers prior to collecting their biometrics, which allows consumers the opportunity to make an *informed* choice when private entities request their biometrics. So, unlike other statutes that only create a right of action if there is a qualifying data breach, BIPA strictly regulates the manner in which entities may collect, store, and use biometrics and creates a private right of action for lack of statutory compliance.

12. In this case, notwithstanding the clear and unequivocal requirements of the law, Defendant disregards Illinois citizens' statutorily protected privacy rights and unlawfully collects, stores, disseminates and uses individual's biometric identifiers and biometric information by electing to implement an invasive biometric face scanning program that relied on the illegal collection of consumers' biometrics, thereby invading their substantive privacy rights under BIPA.

13. Defendant implemented this biometric face scanning regime collecting facial geometry of its customer's potential clientele/consumers without first obtaining consumers' informed written consent and informing such persons how long they planned on keeping such information, as required by law, and all while disregarding the relevant Illinois BIPA and the privacy interests it seeks to protect.

14. Defendant's conduct is particularly unsettling considering the fact that this extremely sensitive biometric information is also associated with consumers' government-issued identification documents. Despite the sensitive nature of this biometric information, Defendant wholly avoids any costs associated with implementing its biometric identity and age verification system in compliance with the law.

15. The Illinois Legislature has found that "biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, even sensitive information like Social Security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to each individual and therefore, once compromised, such individual has no recourse, is at a heightened risk for identity theft in, and is likely to withdraw from biometric facilitated transactions." 740 ILCS 14/5. The risk is compounded when, like in this case, a person's biometric information is also associated with government issued or other photo identification and related information.

16. Plaintiff brings this action for damages and other legal and equitable remedies resulting from the illegal actions of Defendant in capturing, collecting, storing, using, and transmitting his biometrics, and those of thousands of consumers throughout the state of Illinois, without informed written consent, and without informing them through a publicly available written policy of how it was going to store and dispose of this irreplaceable information, in direct violation of the Illinois BIPA.

17. Defendant failed to obtain the necessary consent to handle Plaintiff's and other consumers' biometrics; failed to maintain a lawful biometric storage program which deletes biometric information in the proscribed period; failed to provide the required disclosures at the time of collection; and failed to provide a retention and destruction schedule.

18. To the extent Defendant is still retaining Plaintiff's biometrics, such retention is unlawful and an ongoing infringement of his right to privacy regarding his biometrics as afforded by the BIPA. Plaintiff would not have provided his biometrics to Defendant had he known that Defendant would retain such information for an indefinite period without his consent.

19. On behalf of himself and the proposed Class defined below, Plaintiff seeks an injunction requiring Defendant comply with BIPA, as well as an award of statutory damages to the Class, together with costs and reasonable attorneys' fees.

PARTIES

20. Defendant Jumio Corporation is a Delaware corporation that conducts business, and is licensed by the Illinois Secretary of State to conduct business, throughout Illinois and in Cook County. Jumio transacts business throughout the state of Illinois and knowingly transacts with Illinois residents.

21. At all relevant times, Plaintiff has been a resident and citizen of the state of Illinois.

JURISDICTION AND VENUE

22. This Court has diversity jurisdiction under 28 U.S.C. § 1332(d), because (i) at least one member of the putative class is a citizen of a state different from any Defendant, (ii) the amount in controversy exceeds \$5,000,000 exclusive of interests and costs, and (iii) none of the exceptions under that subsection apply to the instant action.

23. This Court has personal jurisdiction over Defendant because Defendant transacts business in Illinois and because a substantial part of the events giving rise to Plaintiff's claims arise out of Defendant's unlawful in-state actions, as Defendant captured Plaintiff's biometrics in this State.

24. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events giving rise to Plaintiff's claims occurred in this District, as Defendant captured Plaintiff's biometrics in this District.

FACTUAL BACKGROUND

25. Defendant develops and sells and/or licenses its identity verification technologies to companies that sell age-restricted consumer products over the internet as well as to other companies which require identity verification technologies.

26. Defendant openly acknowledges that it uses "advanced technology including biometric facial recognition, machine learning, and verification experts[.]"¹

27. In order to allow Plaintiff to access and potentially purchase age restricted products on one of its customers' websites, Defendant required Plaintiff to use its NetVerify system in Illinois to capture his biometrics in order to verify his age and identity. After requiring Plaintiff to upload a photo of his government issued ID, Defendant took a biometric scan of Plaintiff's face via its NetVerify system and then allowed Plaintiff to have access to its customer's eCommerce platform so that he could access and potentially purchase certain products.

28. On December 19, 2019 Defendant, using its NetVerify "ID & Age Verification System" and the camera on Plaintiff's smartphone captured, collected, stored, and transferred the biometric facial geometry and related biometric information of Plaintiff in Illinois in violation of the BIPA.

29. Prior to taking Plaintiff's biometrics, Defendant did not seek, and Plaintiff never provided, any written consent relating to the collection, use, storage, or dissemination of his biometrics.

¹ <https://www.jumio.com/trusted-identity/netverify/> (last visited December 21, 2018).

30. Defendant subsequently disseminated Plaintiff's biometric information to third parties without his express consent.

31. Prior to taking Plaintiff's biometrics, Defendant did not make publicly available a written policy as to a biometric retention schedule and guidelines for permanently destroying the collected biometrics which was compliant with BIPA or which was available on its customers' websites where Defendant's NetVerify system was deployed. As such, even if Defendant's privacy policy were compliant with the law, Plaintiff could not have reasonably been expected to view such privacy policy prior to Defendant's collection and capture of his facial geometry and related biometric information.

32. To this day, Plaintiff is unaware of the status of his biometrics obtained by Defendant. Defendant has not informed Plaintiff whether it still retains his biometrics, and if it does, for how long it intends to retain such information without his consent.

33. Plaintiff has suffered pecuniary damages in the form of diminution in the unique identifying value of his biometrics, and other costs associated with identity protection and account monitoring.

34. Furthermore, Plaintiff's biometrics are economically valuable and such value will increase as the commercialization of biometrics continues to grow. Defendant's use of Plaintiff's biometrics does and will continue to confer a benefit on Defendant at the expense of Plaintiff's privacy rights.

35. As a result of Defendant's conduct, Plaintiff experiences severe mental anguish, anxiety, and other physical and mental injury when he thinks about the status of his biometrics and who has, or could have, access to such private information; what would happen to his biometrics if Defendant went bankrupt or otherwise sold its assets; whether Defendant will ever delete his

biometric information; what would happen if Defendant or its customers were to experience a data breach, and how any such breach would result in irreparable harm to the security of his identity. This harm is even more acute because an individual or entity with access to Plaintiff's biometrics could potentially access his other financial accounts or health records which may currently, or at some time in the future, be secured through his biometrics.

36. By failing to comply with BIPA, Defendant has violated Plaintiff's substantive state rights to biometric information privacy.

CLASS ALLEGATIONS

37. Pursuant to Rule 23(a) and 23(b) of the Federal Rules of Civil Procedure, Plaintiff brings this action on behalf of himself and a class of similarly situated individuals pursuant to BIPA, 740 ILCS 14/1, *et seq.*, to recover statutory penalties, prejudgment interest, attorneys' fees and costs and other damages owed.

38. As discussed *supra*, Section 14/15(b) of BIPA prohibits a company from, among other things, collecting, capturing, purchasing, receiving through trade, or otherwise obtaining a person's or a customer's biometric identifiers or biometric information, unless it first (1) informs the individual in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the individual in writing of the specific purpose and length of time for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information. 740 ILCS 14/15.

39. Plaintiff seeks class certification under Rule 23 of the Federal Rules of Civil Procedure for the following class of similarly-situated under BIPA:

All individuals whose biometrics were captured, collected, stored, used, transmitted, or disseminated by Defendant Jumio within the State of Illinois at any time within the

applicable limitations period.

40. Excluded from the Class are any members of the judiciary assigned to preside over this matter; any officer or director of Defendant and any immediate family member of such officer or director.

41. Upon information and belief, there are thousands of members of the Class, making the members of the Class so numerous that joinder of all members is impracticable. Although the exact number of members of the Class is currently unknown to Plaintiff, the members can be easily identified through Defendant's records.

42. Plaintiff's claims are typical of the claims of the Class he seeks to represent, because the factual and legal bases of Defendant's liability to Plaintiff and the Class is the same, and because Defendant's conduct has resulted in similar injuries to Plaintiff and to the Class. As alleged herein, Plaintiff and the Class have all suffered damages as a result of Defendant's BIPA violations and various common law transgressions.

43. There is a well-defined commonality of interest in the substantial questions of law and fact concerning and affecting the Class in that Plaintiff and all members of the Class have been harmed by Defendant's failure to comply with BIPA. The common questions of law and fact for the Class include, but are not limited to, the following:

- a. Whether Defendant made available to the public a written policy that establishes a retention schedule and guidelines for destroying biometrics;
- b. Whether Defendant obtained a written release from the Class before capturing, collecting, or otherwise obtaining their biometrics;
- c. Whether Defendant provided a written disclosure to the class that explains the length of time their biometrics stored and used before taking their biometrics;

- d. Whether Defendant's conduct violates BIPA;
- e. Whether Defendant's violations of the BIPA are willful or reckless; and
- f. Whether Plaintiff and the Class are entitled to damages and injunctive relief.

44. Plaintiff will fairly and adequately represent and protect the interests of the other members of the Class he seeks to represent. Plaintiff has retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the other members of the Class and have the financial resources to do so. Neither Plaintiff nor his counsel has any interest adverse to those of the other members of the Class.

45. Defendant has acted and failed to act on grounds generally applicable to the Plaintiff and the other members of the Class, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the members of the Class and making injunctive or corresponding declaratory relief appropriate for the Class as a whole.

46. The common questions identified above predominate over any individual issues, which will relate solely to the quantum of relief due to individual class members. A class action is superior to other available means for the fair and efficient adjudication of this controversy because individual joinder of the parties is impracticable. Class action treatment will allow a large number of similarly-situated persons to prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of effort and expense if these claims were brought individually. Moreover, as the damages suffered by each class member are relatively small in the sense pertinent to class action analysis, the expenses and burden of individual litigation would make it difficult for individual class members to vindicate their claims.

47. Additionally, important public interests will be served by addressing the matter as a class action. The cost to the court system and the public for the adjudication of individual litigation and claims would be substantially more than if claims are treated as a class action. Prosecution of separate actions by individual class members would create a risk of inconsistent and varying adjudications, establish incompatible standards of conduct for Defendants, and/or substantially impair or impede the ability of class members to protect their interests. The issues in this action can be decided by means of common, class-wide proof. In addition, if appropriate, the Court can and is empowered to fashion methods to efficiently manage this action as a class action.

COUNT I

**Violations of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.*,
(On behalf of Plaintiff and the Class)**

53. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

54. Defendant is a private entity under BIPA.

55. Plaintiff and the Class members had their biometric identifiers and/or their biometric information collected, captured, received or otherwise obtained and/or used by Defendant (in the form of facial geometry). *See* 740 ILCS 14/10.

56. Plaintiff's biometric identifiers were used to identify him, and, therefore constitute "biometric information" as defined by BIPA. *See* 740 ILCS 14/10

57. Defendant captured, collected, stored, and/or used Plaintiff's and the Class members' biometrics without informed written consent and without complying with BIPA through its biometric identity and age authentication software.

58. Upon information and belief, Defendant Jumio disclosed Plaintiff's biometric identifiers and/or biometric information to at least one third party without his informed written consent.

59. Plaintiff and the Class members have been aggrieved by Defendant's failures to adhere to the following BIPA requirements, with each such failure constituting a separate and distinct violation of BIPA:

- a. Defendant failed to inform Plaintiff and the Class members in writing that their biometrics were being collected and stored, prior to such collection or storage, as required by 740 ILCS 14/15(b)(1);
- b. Defendant failed to inform Plaintiff and the Class members in writing of the specific purpose for which their biometrics were being captured, collected, stored, and used, as required by 740 ILCS 14/15(b)(2);
- c. Defendant failed to inform Plaintiff and the Class members in writing of the specific length of term their biometrics were being captured, collected, stored, and used, as required by 740 ILCS 14/15(b)(2);
- d. Defendant failed to obtain a written release from Plaintiff and the Class members, as required by 740 ILCS 14/15(b)(3);
- e. Defendant failed to provide a publicly-available retention schedule detailing the specific length of time the biometrics are stored and/or guidelines for permanently destroying the biometrics it stores, as required by 740 ILCS 14/15(a); and
- f. Defendant failed to obtain informed consent to disclose or disseminate the Class members' biometrics, as required by 740 ILCS 14/15(d)(1).

60. By capturing, collecting, storing, using, and disseminating Plaintiff's and the Class members' biometrics as described herein, Defendant denied Plaintiff and the Class members their

right to statutorily-required information and violated their respective rights to biometric information privacy, as set forth in the BIPA.

61. Plaintiff's and the Class's biometric information have been and will continue to be unlawfully accessed by third parties.

62. Had Defendant informed Plaintiff that he was not being provided with the required information regarding his biometrics and the biometric face scanning program as required by law, he would not have provided his biometrics to Defendant.

63. Had Defendant informed Plaintiff that he would be asked to participate in an illegal biometric face scanning program, Plaintiff would not have used Defendant's biometric face scanning system, or he at least would have been able to make an informed decision concerning material facts of his use of the NetVerify "ID & Age Verification System," including whether the benefit justifies the increased risk in participating in Defendant's unlawful biometric program.

64. BIPA provides for statutory damages of \$5,000 for each willful and/or reckless violation of BIPA and, alternatively, damages of \$1,000 for each negligent violation of the BIPA.

65. Defendant's violations of BIPA, as set forth herein, were knowing and willful, or were at least in reckless disregard of the statutory requirements. Alternatively, Defendant negligently failed to comply with the BIPA disclosure, consent, and policy posting requirements.

66. Accordingly, with respect to Count I, Plaintiff, on behalf of himself and the proposed Class, prays for the relief set forth below.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the proposed Class, respectfully requests that this Court enter an Order:

- a. Certifying the Class as defined above, appointing Plaintiff as class representative and the undersigned as class counsel;
- b. Declaring that Defendant's actions, as set forth herein, violate the BIPA;
- c. Awarding injunctive and equitable relief as necessary to protect the interests of Plaintiff and the Class by requiring Defendant to comply with the BIPA requirements for the capture, collection, storage, use, and dissemination of biometric identifiers and biometric information;
- d. Awarding statutory damages of \$5,000 for each willful and/or reckless violation of the BIPA, pursuant to 740 ILCS 14/20(1);
- e. Awarding statutory damages of \$1,000 for each negligent violation of the BIPA, pursuant to 740 ILCS 14/20(3);
- f. Awarding reasonable attorneys' fees, costs, and other litigation expenses pursuant to 740 ILCS 14/20(3);
- g. Awarding pre- and post-judgment interest, as allowable by law; and
- h. Awarding such further and other relief as the Court deems just and equitable.

JURY DEMAND

Plaintiff requests trial by jury of all claims that can be so tried.

Dated: April 15, 2019

Respectfully Submitted,

ALEX PRELIPCEANU, individually and on
behalf of a class of similarly situated individuals

By: /s/ David Gerbie
One of Plaintiff's Attorneys

Myles McGuire
David L. Gerbie
Jad Shekali
MCGUIRE LAW, P.C. (Firm ID: 56618)
55 W. Wacker Drive, 9th Fl.
Chicago, IL 60601
(312) 893-7002
Fax: (312) 275-7895
mmcguire@mcgpc.com
dgerbie@mcgpc.com
jsheikali@mcgpc.com

Attorneys for Plaintiff and the Putative Class

CERTIFICATE OF SERVICE

I hereby certify that on April 15, 2019, I caused the foregoing *First Amended Complaint* to be electronically filed with the Clerk of the Court using the CM/ECF system. A copy of said document will be electronically transmitted to all counsel or record.

/s/ David L. Gerbie